Title	Version	Replaces	Org. location	Page # (of #)
Policy for Information and Data	1.4	1.3	N/A	1(4)

Owner	Changed by	Latest changed	Document type
CFO	Tova Boustedt	2025-04-22	Policy

Adopted by	Adopted on (Date)	Status	Replaced by
The Board of Directors	2025-05-06	Adopted	N/A

Policy for Information and Data

Background

What does this policy include?

This policy outlines Hemnet Group AB (publ) and its subsidiaries (the “Company", the “Group") approach to managing and protecting its information and data assets. The policy aims to ensure that Hemnet upholds the integrity, confidentiality, and availability of its information assets while complying with legal requirements and best practices. Furthermore, it addresses the risks associated with information security and data privacy, establishing clear guidelines for responsible data management, access controls and incident handling.

Who is affected by this policy?

This policy applies to all employees, hires and consultants at the Company who have in any way been trusted with and given access to Hemnet's data and information assets.

Why have we created this policy?

The core objectives of this policy are to ensure that data is collected, handled, and protected in compliance with applicable data protection laws while safeguarding the integrity, confidentiality, and availability of our information assets. It aims to protect Hemnet's operations, reputation, and the individual's right to personal privacy by implementing risk-based security measures. The policy also ensures compliance with General Data Protection Regulation (GDPR), promotes responsible data management, and establishes clear procedures for access control and incident handling.

Information

Hemnet’s overall goal for information and data

Data is an important asset for our business, and we use our data to develop our business and our operations. The use of Hemnet’s data must always comply with applicable laws and take into account the interests of affected individuals’ personal privacy.

Using a risk-based approach, Hemnet will use relevant security measures to protect the business from any form of threat to information systems or data that may interfere with or adversely affect the Company’s business, the reputation or the individual's right to personal privacy. This includes risks that can affect the Company’s information systems and its integrity, confidentiality and accessibility of our data.

Focus

- Hemnet will use all reasonable measures we can to protect and manage our data in a manner that follows applicable data protection legislation as well as our stakeholders' requirements and reasonable expectations. Safeguards shall be designed to include, but not be limited to, availability, confidentiality and integrity.

- All safeguards should, as far as possible, be based on good practice (ex. ISO 27001/27701). When choosing and implementing protective measures, consideration should be given to the impact on the Company’s employees and visitors.
- Appropriate measures shall be taken to ensure the security of physical information assets. These assets include, but are not limited to, the company's offices, computers, networking equipment, and storage devices.
- The Company shall continuously and systematically work on analysing and evaluating the requirements, expectations and risks that exist in our information and data to ensure that the measures taken are relevant and effective. The evaluation shall be conducted in accordance with the guidelines established by the Company's senior executive management team.
- There should be relevant guidelines and procedures for the protection of personal data to ensure that the Company complies with applicable data protection legislation.
- From collection to deletion, the Company must ensure that the data is accurate and trustworthy.
- All information and data assets must be documented, and all assets must be assigned a classification to ensure that they are properly managed.
- In all development work and procurement, the protection of personal data and information security must always be part of the requirements.
- All employees who handle incidents related to information and data should have sufficient knowledge to determine if an incident includes personal information.
- All employees who handle personal data must have sufficient knowledge of the regulations governing personal data processing.
- The Company shall have relevant procedures to deal with all types of incidents arising from identified risks.
- For important information and data assets, there must be a continuity plan that ensures that the business can continue in the event of serious disruptions in accessibility.
- Hemnet shall assign access to information and IT resources only to the extent necessary to enable the execution of assigned tasks, in accordance with the principles of minimum possible access.
- Any person assigned access, eg. in the form of account details, shall be aware that the assignment is personal and may not be made available to another party regardless of its relation to Hemnet or in any way transferred without the prior approval from the function that assigned the access.
- The Company should strive for a culture of high awareness of information security and protection of personal dataAll employees, regardless of form of employment, should be aware of the rules and guidelines that apply to data and information systems and understand the importance of responsible use of the Company's data and information assets.

Governance

Roles and Responsibilities

This policy is owned by the CFO with any updates or amendments requiring approval from the Board of Directors. Senior management and the Board are responsible for ensuring that data protection and

information security are upheld in accordance with this policy. To ensure that the Company's use of information, information systems, and data aligns with business objectives, the senior executive management team shall also be responsible for maintaining clear governance of Hemnet's strategic decisions and investments. This includes ensuring that roles, responsibilities, and powers are clearly documented in accordance with the IT Governance Guidelines. All individuals with access to Hemnet's resources must adhere to this policy and report any potential violations.

Third Party Standards

Hemnet operates in alignment with internal principles, strategic priorities, and key regulatory requirements (e.g., GDPR).

Follow-up and compliance

Monitoring and Review

This Policy undergoes an annual review in accordance with Guidelines for Hemnet's Steering Document and the Policy for Corporate Governance, to ensure its proper implementation and continued relevance to Hemnet's operational needs. During the review, it is assessed for effectiveness in addressing current risks and compliance requirements.

The review process is conducted by the HOIS in accordance with Hemnet's Policy for Corporate Governance. The HOIS ensures the policy remains aligned with regulatory changes, evolving business needs, and ensures compliance through appropriate supporting documents and training. The results of the review process, including any necessary updates, are reported to the Board of Directors for final approval.

Policy Accessibility

This policy is accessible to all employees and relevant stakeholders through internal communication platforms and Hemnet's corporate website at https://www.hemnetgroup.se/. Training and educational materials are provided to ensure comprehensive understanding and adherence to the policy.

Reporting channels for compliance issues

Hemnet's Code of Conduct indicates which reporting channels are to be used by employees who detect violations in compliance with Hemnet's steering documents. Each employee is asked to raise compliance issues with the person concerned in the matter in the first place where possible. If it is not suitable or possible, the employee should contact the immediate supervisor. If that is also not suitable or possible, employees are asked to contact their supervisor's supervisor, Hemnet's Chief People & Culture Officer or Hemnet's General Counsel. Also, severe misconduct can be reported anonymously via the Company's whistleblower function available via https://report.whistleb.com/en/hemnet.

Violations of this policy

Violations of this policy will always be taken very seriously and may lead to disciplinary action, including dismissal. In addition, violation of relevant laws may mean that you (and/or the Company) are subject to legal sanctions.

Related documents

- Guidelines for Data Safety
- Guidelines for information security
- Guidelines for information classification
- Guidelines for responsible use
- Guidelines for responsibility and authority IT
- Guidelines for choice of suppliers
- Guidelines for Hemnet’s Steering Documents.
- Code of Conduct